Protection of information technology facilities

CFPA-E Guideline No 14:2019 F

CFPA EUROPE

European Guideline

FOREWORD

The European fire protection associations (CFPA-E) have decided to produce common guidelines in order to achieve similar interpretation in European countries and to give examples of acceptable solutions, concepts and models. The Confederation of Fire Protection Associations in Europe (CFPA E) has the aim to facilitate and support fire protection work in European countries.

The objectives of CFPA Europe are to improve safety and security and to prevent the consequent loss of life, destruction of property and disruption to business activities. CFPA Europe also seeks to meet the increasing demands for quality and safety in the workplace.

This guideline concerns IT systems, the most important facilities of companies, regardless of their size. The recommended measures in this guideline are intended to minimize hazards resulting from the operation site and its surroundings, in order to ensure the necessary availability of IT systems and their safe operation. Therefore, the present guideline is addressed to IT planners, IT manager of companies and organization including external service providers.

The proposals on which this guideline is based were produced by German Insurance Association (GDV). Herewith, the former guideline on fire protection in information technology facilities (CFPA-E No. 14:2007 F) is extended to all typical hazards from the surroundings of IT operational site.

The Guideline has been compiled by the Guidelines Commission and adopted by all fire protection associations in the Confederation of Fire Protection Associations Europe.

These guidelines reflect best practice developed by the countries of CFPA Europe. Where the guidelines and national requirements conflict, national requirements must take precedence.

Copenhagen, March 2019 CFPA Europe	Madrid, March 2019 Guidelines Commission
Jesper Ditlev Chairman	Miguel Vidueira Chairman

CFPAEUROPE®

Contents

1. Scope

In the present guideline, typical hazards that IT systems can be exposed in a company site are called regardless of the type of business. Accordingly, measures to minimize these hazards and the associated risks for a concerning company and its operation are recommended, depending on the risk assessment and required availability.

The recommendations can also apply to other organizations.

Issues such as cybercrime and software requirements including legal liability and insurance aspects are not treated.

2. Introduction

IT systems in businesses are becoming increasingly important. This can be recognized inter alia at increasing automation of workflows, increasingly complex operating processes with high technical demands, increasing electronic exchange of information and rapid technological change. At the same time the failure of IT systems and thus possibly associated data loss can affect the companies and their operating significantly. These risks must be accordingly covered by risk management and should be controlled by a holistic protecting concept.

3. Definitions

The subsequent terms are used for the present guideline.

Availability
Ratio of the time within an agreed period, in which the system for its intended purpose is operationally available (operating time).

Note: The operating time can be limited by regular servicing, failure, damage, as well as repairs to correct them.

IT systems

Generic term of all installed facilities for electronic data processing except individual PC.

Protection level
Degree for the necessary measures to ensure the necessary availability and to control the associated risks.

4. Typical hazards and risks

Due to the scope of this guideline, IT systems in companies can be generally exposed to the following hazards

- Failures by the building facilities, e. g. electrical systems, heating, air conditioning / ventilation, water supply
- Fire and smoke
- Natural hazards, e. g. lighting, flood, storm, heavy rain, snow pressure, earthquake
- Other hazards from neighbourhood and operational processes
- Burglary, sabotage and vandalism

In case of a realization of these risks IT systems can fail and the operational process can therefore be seriously affected and even interrupted.

Is the failure of IT systems connected to a data loss, business interruption may possibly be worse, because valuable resources of the company are bound for a long time for data recovery. The loss of customer data is also connected with a loss of image, when customer concern about the dealing with his personal data and their security.

5. Protective concept and level

In order to limit the variety of hazards and to control the associated risks, a holistic protective concept has proven itself in practice. In it, necessary protective measures are summarized in respect to the object-specific features that should be planned and implemented in accordance. This makes it possible, such measures preferred to use, which can cover multiple hazards in general, and optimize therefore the protection technically and economically.

Table 1 Exemplary Assignment of protection levels

IT Facilities	**Necessary availability**		
	Low / Normal	**Middle**	**High**
Single server	**I**	**I**	**II**
Server room	**I**	**II**	**III**
Data centre	**II**	**III**	**III**

The table above shows the protection level as example, depending on the required availability and used IT systems. With this classification, the practice should be supported in their decision, which effective protective measures in necessary extent should be taken. The classification of availability can be made each by the operators of IT systems in accordance with the definition of availability.

Another differentiation of IT systems in terms of their significance for a company and its operation is always possible. For IT systems, for which a very high availability is required, additional measures beyond this guideline may be needed.

6. Protection measures

In subsequent sections, protection measures are exemplary listed as guidance and with respect to the hazards and protection levels (see section 5). Here, IT systems with a necessary protection level III need, if applicable, to take all recommended measures of protection level I to III, IT systems with a necessary protection level II need, if applicable, to take all recommended measures of protection level I to II. They do not replace the required consideration in each individual case.

For planning and, if necessary, dimensioning of the recommended measures, relevant codes that are available both European and nationally, are to take into account.

6.1 General

The following protective measures should be generally implemented for all IT systems:

6.1.1 Protection level I

- Ban the use of non-operating electrical devices such as coffee machines and refrigerators or including these devices in the regular inspection
- Implementation of the smoking ban Instruction and regular training of employees on fire protection
- Implementation of hot work permit procedure with introduction of persons that are involved in hot work, including employees of foreign companies
- Using of self-extinguishing waste containers in the IT rooms
- Establish and updating a site-related Fire Safety Regulations
- Regular instruction on appropriated behaviour in case of operational disturbances
- Regular servicing by trained personnel in accordance with the specification of manufacturer's or installer
- Regular inspection by recognized professionals
- Immediate elimination of errors and defects by specialist companies
- Regular site inspection with respect to fire protection, include visual checks of electrical installation for visible damage, in order to avoid electric-related causes of damage
- For the planning, installation and supporting appropriate specialist and companies should be commissioned, also for comprehensive documentation; complex task should be coordinated by a project manager.

6.1.2 Protection level II

- Physical separation of different DP (data processing) areas such as rack/server, backup, operator, printers, emergency/UPS, supply technology including extinguishing systems, in order to avoid a mutual adverse effect, to protect important elements of the IT facilities and to minimize downtime in case of destruction of a DP-block
- Dispose of all waste from the IT rooms, in order to reduce fire loads
- Maintenance (servicing, inspection and repair): Assignment of an IT security officer who should check and monitor the compliance with the established and implemented protection concept including regular maintenance, its commissioning and documentation.

6.1.3 Protection level III

- See hazard-related notes.

6.2 Electrical systems

Hazards in electrical installation have many and different causes. Measures to prevent or to limit these hazards and associated risks are often covered by standards. From these reasons, typical hazards and the general objectives of protective measures are listed in the following. The concrete fixing of necessary measures can be carried out in accordance with the agreed protection level and relevant standards and depending on present hazards and objectives.

Hazards

- Lightning or similar surges, e. g. switching surges or tripped circuit breaker
- Arcing in main distribution and arcing fault in final circuit
- Failure of a medium-/low-voltage feed, failure of the inlet by fire
- Influences from the supply network, by own installations or from the data line
- Interference from own network (current to the protective conductor)
- Voltage differences of ground potential
- Voltage spike
- Overvoltage caused by electric fields
- Deactivation of residual current circuit breaker, caused by short time anomalies of network
- Insufficient overcurrent protection of sockets, especially provisional multiple sockets.

General objectives:

- Derivation of possible lightning currents
- Securing the energy supplies by separate and redundant power supply and therefore the continuity of operation, second independent power supply possibly with emergency generators and taking the supply-time and other technical constraints into account
- Avoiding
  - interference from one's own electrical network (power to the protective conductor)
  - interference from one’s own installation (electromagnetic compatibility)
  - interference from voltage differences and other interferences in complex IT systems and
  - transient currents on data line screens;
- Protection against
  - short high voltage pulses
  - network-related voltage peaks or harmonics waves
  - overvoltage caused by electric fields
- Minimize potential impact of a short circuit
- Early identification and localization of interference sources
- Maintenance of function over a period of time in spite of fire, e. g. using the function integrity and installation of the second conduction path through other fire compartments

6.3 Failures of other building facilities (Heating, ventilation/air condition, water pipe)

The measures in this sub section relate to the following aspects:

- General: Get the redundancy for continued operation of mission-critical supply engineering in case of failure and decoupling of energy technology from the primary DP-operation
- Overheating: Avoid an temperature stress of the DP facilities, additional source of ignition and the occurrence of condensation
- Ventilation / air condition: Avoiding the aspiration of polluted air, e. g. exhaust air; avoid the spread of smoke in case of fire
- Water pipe: Preventing the accumulation or water ingress into the server room in case of leakages or backwater; Discharging and detection of entered liquids

In case of critical operation state, emergency stop switch should be installed in systems of building facilities with consideration of possible consequences for the IT system, in order to avoid damage, e. g. by smoke.

6.3.1 Protection level I

- General: Integration of key technology equipment into the surveillance by fire detection system and protection by fire extinguishing system
- Overheating:
  - Monitor the server temperature, at least with malfunction message
  - Installation of stationary cooling / ventilation systems (No provisional solution)
  - Ensure the orderly shutdown of the computer
- Ventilation /air condition: Activate fire dampers with the characteristic smoke
- Water pipe: Avoiding electrical connectors in moisture hazard area and elevation of IT facilities approx. 12 cm above ground (e. g. due to inventory insurance conditions).

6.3.2 Protection level II

- General: Constructional separation between server room and other IT facilities with ceilings and walls including closures of operational needed openings that have a classified fire resistance of 90 minutes
- Overheating: No special measure
- Ventilation / air condition:
  - monitor the extraction and inlet air (especially in recirculation mode) by appropriate fire detection
  - shutdown of the ventilation system in case of fire detection
- Water pipe:
  - Laying of fresh or waste water outside the server room
  - No openings to sewer or installation of backflow valves
  - Monitoring of floor leakage in rooms with IT facilities.

6.3.3 Protection level III

- General: Redundant design of essential services (e. g. air, cooling) with fire-resistant separation to each other
- Overheating: Redundant monitoring of the ambient temperature with malfunction message
- Ventilation / air condition:
  - The fresh air intake must not be affected
  - Use non-combustible insulation materials, especially by exhaust air ducts
  - Arrangement of aspiration for outdoor air on the roof and at the leeward side; considering the neighbourhood
  - Integration of ventilation systems including the ventilation / air condition centre into the protection with inerting system, if present;

- Water pipe:
  - Preparation of the server room including double bottom with gradient and collecting chamber / pump sump for liquids
  - No water pipes above the server room ceiling or construction of a water barrier in or beneath the server room ceiling
  - Laying unavoidable fluid pipes in double pipes.

6.4 Fire and smoke

The measures in this sub section relate to the following aspects

- General
- Ignition and fire development
- Fire spread
- Smoke spread
- Fire detection and suppression

In addition to following recommendations, an exemplary checklist is contained in the appendix. Also recommendations of GL No. 25:2010 F "Emergency Plan" should be followed.

Some of the recommendations below have been left intentionally in blank to stimulate reflection about the best practice to apply.

6.4.1 Protection level I

- General: Arrangement of rooms with DP in areas with low fire hazards, e. g. low fire loads
- Ignition and fire development: -
- Fire spread: Separation of rooms with DP to adjacent rooms through separating elements with a classified fire resistant of 90 min
- Smoke spread: Separation of rooms with DP to adjacent rooms through separating elements with tightly closing closures
- Fire detection and suppression: Installation of appropriate fire extinguishers (CO2 for electrical installations, foam / water for office areas)

6.4.2 Protection level II

- General: Avoiding dust emissions and deposits, especially in the server room
- Ignition and fire development: Using non-combustible construction materials for structural components, e. g. cladding, insulation, wall coverings, floor panels
- Fire spread: Separation of rooms with DP to adjacent rooms through separating elements that limit the room temperature facing away from the fire to max. 50 to 60 ° C, after a fire exposure of 90 min
- Smoke spread: Using "low smoke" cable, e. g. bus bar and minimizing PVC cables or protection of the cable with paint, wrapping
- Fire detection and suppression: Installation of appropriate automatic fire detection systems also in raised floors, suspended ceilings and peripheral areas of equipment.

6.4.3 Protection level III

- General: -
- Ignition and fire development: -
- Fire spread: -
- Smoke spread: Maintaining in case of fire a positive pressure in server room with help of air conditioning or ventilation systems, in order to avoid the entrance of smoke
- Fire detection and suppression: Installation of automatic fire extinguishing systems for room protection and, if necessary, installation of (permanent) inerting systems

6.5 Natural hazards

The measures in this sub section relate to the following natural hazards

- Earthquake
- Flood
- Heavy rain
- Landslide
- Storm
- Snow / Ice

These hazards should be considered already in the planning phase, in order to avoid the location with increased natural hazards, such as valley or river area.

6.5.1 Protection level I

- Earthquake: Building in safer construction in accordance with the respective earthquake zone
- Flood: Choosing a installation room with low flood hazards
- Heavy rain: Regular cleaning and maintenance of downpipes (see also note on flood)

- Landslide: -
- Storm: Avoiding or limitation of openable windows in exterior wall of rooms with DP
- Snow / Ice: Avoiding overload by snow and ice, especially on flat roofs with help of timely snow removal and pay attention to the self-assurance of the crew.

6.5.2 Protection level II

- Earthquake: -
- Flood: Installation of water detector in rooms with DP
- Heavy rain: Increased arrangement or protection of the building opening on the ground floor and basement (see also note on flood)
- Landslide: -
- Storm: -
- Snow / Ice: -

6.5.3 Protection level III

- Earthquake: Location of backup computer centre outside the earthquake zone
- Flood: Protection of rooms with DP, e. g.
  - waterproof construction of building parts that are lying in the ground ("white / black try")
  - water pressure-tight cable entries into the building and server room
  - arrangement of openings above the typical flood threshold
- Heavy rain: pay attention to possible water accumulation on flat roofs (see also note on flood)
- Landslide: Avoid location on a slope
- Storm: Avoid installation of technical equipment on the roof and facade, e. g. antennas, directional radio, laser transmitting, receiving devices
- Snow / Ice: Introduction of a snow management system, in order to ensure timely snow removal by
  - Systematic planning including the check of the static
  - commissioning of external experts and companies
  - Arrangement of transportation and storage of snow and ice.

6.6 Other Hazards from neighbourhood and operational processes (Dust, gases and vapours, mechanical vibration and shock, etc.)

In this sub section, measures to avoid mechanical vibration and shock by operational equipment, motor vehicle traffic in the neighbourhood and vehicle impact etc. are called:

6.6.1 Protection level I

- Choosing a safe location inside a building
- Wires are to be provided with protection against rodents, in order to prevent line breakage and failure by nail bite, the.

6.6.2 Protection level II

- Choosing a safe location on the premise.

6.6.3 Protection level III

- Consideration emitting neighbourhood in the choice of site location, e. g. sandy areas, such as sports fields, coastal waters, industrial enterprises and processing, in order to avoid the risks of data processing by critical emissions
- Choosing a premise with low hazards of interferences

6.7 Data losses

The measures in this sub section relate to the following hazards:

- Defect of hardware
- Failure of backup
- Failure of data medium
- Failure of IT Responsible

6.7.1 Protection level I

- Defect of hardware: Provision on external backup computer
- Failure of backup: check the backups, regular performing of test, exercising of restore, establishing and update the plan for backups
- Failure of data medium: Decentralized storage of backups
- Failure of IT Responsible: -

6.7.2 Protection level II

- Defect of hardware: Separating of redundant data and DP centre with fire protection separation (as a separate fire compartment) and independent supply engineering
- Failure of backup: -

- Failure of data medium: Storage on different data media
- Failure of IT Responsible: establishing and update an emergency plan.

6.7.3 Protection level III

- Defect of hardware: -
- Failure of backup: -
- Failure of data medium: -
- Failure of IT Responsible: Introduction of a representative provision with documentation by describing the system structure and data to other authorized persons as well as deposit of passwords.

7. References

1. European Directive 99/92/EC (sometimes known as the ATEX 137 or ATEX Workplace Directive): Minimum requirements for improving the safety and health protection of workers potentially at risk from explosive atmospheres.

EN 50600: Information technology - Data centre facilities and infrastructures.

VdS CEA 4001: Sprinkler Systems, Planning and Installation

8. Appendix

8.1 Advice on the contents of an internal emergency plan

For further advice on the layout and contents of an emergency plan, please refer to CFPA-E Guideline No. 25:2010 F "Emergency Plan".

8.2 Advice on Security aspects

For a better advice on the Security aspects to consider in IT systems, please refer to CFPA-E Guideline No. 10:2016 S "Protection of Business Intelligence".

8.3 Checklist example

The following table is given as an example of the different fire safety aspects to be checked for evaluation of IT systems.

	Yes	No	Not relevant
Tidiness and cleanliness in the IT facility/Organisation			
The IT facility is devoid of furniture and other objects.			
Waste and packaging materials are removed on a regular basis.			
The smoking ban is complied with.			
Fire drills have been carried out.			
No private electrical devices are available in the IT facility rooms.			
Electrical system/Lightning and overvoltage protection			
No combustible materials are stored near electrical distributors, switchgear or battery			
Only authorised devices are in operation.			
Compulsory inspections of the lightning and overvoltage protection system have been carried out.			
Fire and smoke doors			
The doors are functional (closing device not wedged).			
Doors are freely accessible (not blocked, e.g. by stored goods)			
Openings in fire compartment walls and ceilings			
Have all cable and pipe ducts been sealed appropriately?			
Have ducts in the construction site area been sealed provisionally?			
Manual extinguishing equipment			
All fire extinguishers and wall hydrants are freely accessible.			
Fire extinguishers are inspected on a regular basis and positioned appropriately.			
Hot works			
The safety procedure for hot works has been applied at all times.			
Fire detection and fire extinguishing systems			
Regular maintenance and inspection works have been carried out.			
The systems are operational; e.g. no detectors have been disabled.			
Alarms/emergency calls			
The emergency call system is operational.			
The voice alarm system is operational.			
Intercoms (e.g. in lifts) can be used for emergency calls.			
Emergency organisation			
Emergency call lists and emergency plans are up to date.			

Emergency instructions for reception desks and plant protective forces/security guards are up to date.			

9. European guidelines

Fire

Guideline No.	1:2015 F	-	Fire protection management system
Guideline No.	2:2013 F	-	Panic & emergency exit devices
Guideline No.	3:2011 F	-	Certification of thermographers
Guideline No.	4:2010 F	-	Introduction to qualitative fire risk assessment
Guideline No.	5:2016 F	-	Guidance signs, emergency lighting and general lighting
Guideline No.	6:2011 F	-	Fire safety in care homes for the elderly
Guideline No.	7:2011 F	-	Safety distance between waste containers and buildings
Guideline No.	8:2004 F	-	Preventing arson – information to young people
Guideline No.	9:2012 F	-	Fire safety in restaurants
Guideline No.	10:2008 F	-	Smoke alarms in the home
Guideline No.	11:2015 F	-	Recommended numbers of fire protection trained staff
Guideline No.	12:2012 F	-	Fire safety basics for hot work operatives
Guideline No.	13:2015 F	-	Fire protection documentation
Guideline No.	14:2019 F	-	Protection of information technology facilities
Guideline No.	15:2012 F	-	Fire safety in guest harbours and marinas
Guideline No.	16:2016 F	-	Fire protection in offices
Guideline No.	17:2015 F	-	Fire safety in farm buildings
Guideline No.	18:2013 F	-	Fire protection on chemical manufacturing sites
Guideline No.	19:2009 F	-	Fire safety engineering concerning evacuation from buildings
Guideline No.	20:2012 F	-	Fire safety in camping sites
Guideline No.	21:2012 F	-	Fire prevention on construction sites
Guideline No.	22:2012 F	-	Wind turbines – Fire protection guideline
Guideline No.	23:2010 F	-	Securing the operational readiness of fire control system
Guideline No.	24:2016 F	-	Fire safe homes
Guideline No.	25:2010 F	-	Emergency plan
Guideline No.	26:2010 F	-	Fire protection of temporary buildings on construction sites
Guideline No.	27:2011 F	-	Fire safety in apartment buildings
Guideline N0.	28:2012 F	-	Fire Safety in laboratories
Guideline No.	29:2013 F	-	Protection of paintings: Transport, exhibition and storage
Guideline No.	30:2013 F	-	Managing fire safety in historical buildings
Guideline No.	31:2013 F	-	Protection against self-ignition and explosions in handling and storage of silage and fodder in farms
Guideline No.	32:2014 F	-	Treatment and storage of waste and combustible secondary raw materials
Guideline No.	33:2015 F	-	Evacuation of people with disabilities
Guideline No.	34:2015 F	-	Fire safety measures with emergency power supplies
Guideline No.	35:2017 F	-	Fire safety in warehouses

Guideline No. 36:2017 F - Fire prevention in large tents

Guideline No. 37:2018 F - Photovoltaic Systems: Recommendations on loss prevention

Natural hazards

Guideline No. 1:2012 N - Protection against flood

Guideline No. 2:2013 N - Business Resilience – An introduction to protecting your business

Guideline No. 3:2013 N - Protection of buildings against wind damage

Guideline No. 4:2013 N - Lightning protection

Guideline No. 5:2014 N - Managing heavy snow loads on roofs

Guideline No. 6:2015 N - Forest fires

Guideline No. 7:2018 N - Demountable / Mobile flood protection systems: Recommendations on planning, selection, providing and using.

Security

Guideline No. 1:2010 S - Arson document

Guideline No. 2:2010 S - Protection of empty buildings

Guideline No. 3:2010 S - Security system for empty buildings

Guideline No. 4:2010 S - Guidance on key holder selections and duties

Guideline No. 5:2012 S - Security guidelines for museums and showrooms

Guideline No. 6:2014 S - Emergency exit doors in non-residential premises

Guideline No. 7:2016 S - Developing evacuation and salvage plans for works of art and Heritage buildings

Guideline No. 8:2016 S - Security in schools

Guideline No. 9:2016 S - Recommendation for the control of metal theft

Guideline No. 10:2016 S - Protection of business intelligence